The Internet Archive is under a DDoS attack (archive.org)

230 points by toomanyrichies 5 hours ago | hide | past | favorite | 86 comments

add comment

Simon_ORourke 5 hours ago | next [–]

Why, what's the point in doing such nonsense? Unless it's someone with lots of money, contacts in the dark web, and some historic Barbara Streisand type chip on the shoulder.

reply

somenameforme 4 hours ago | parent | next [–]

DDOS attacks are dirt cheap and can be contracted from large professional sites offering customer support and the works. The largest one taken down had hundreds of thousands of users, and had carried out some 4 million attacks, for prices starting at $14.99/month. [1]

So in other words, anybody can carry out a DDOS for basically no cost. So trying to analyze the purpose, let alone suspects, is probably not going to be fruitful.

[1] - https://wccftech.com/865619-2/

reply

sva_ 1 hour ago | root | parent | next [–]

And they're curiously usually protected by Cloudflare.

reply

neurostimulant 1 hour ago | root | parent | next [–]

Doubt cloudflare has anything to do with it. The operators most likely don't want to openly expose their website's ip addresses.

reply

mike_d 1 hour ago | root | parent | next [–]

That is exactly the problem. These services are constantly at war with each other and are attacked by competitors. Cloudflare provides DDoS protection to the DDoS providers so they can keep their services online, which directly benefits Cloudflare by DDoS being a bigger problem than if they were all busy attacking each other.

This is a sampling of currently available services and who they use for DDoS protection:

```
stresslab.app - Cloudflare
maxstresser.com - Cloudflare
sunnystress.com - Cloudflare
tresser.io - Cloudflare
ip-stresser.net - Cloudflare
hardstresser.com - DDoSGuard
zdstresser.net - Cloudflare
starkstresser.net - Cloudflare
stresserhub.org - Cloudflare
nightmarestresser.net - DDoSGuard
```

Just for fun head over to Cloudflare's abuse reporting site and try to figure out how to get one of these taken down. https://abuse.cloudflare.com/

reply

jsheard 1 hour ago | root | parent | next [–]

DDoSGuard has a reputation for being the Crime CDN, disproportionately serving things like phishing campaigns, black hat forums, piracy sites, etc, so the fact that they are merely the *second* most popular CDN amongst DDOS providers after Cloudflare speaks volumes.

reply

jsheard 1 hour ago | root | parent | prev | next [–]

It's obvious why a DDOS provider would want to use Cloudflare, but their point is that Cloudflare turns a blind eye to DDOS providers using their services. Actively helping to keep DDOS providers online while also selling DDOS mitigation isn't a good look to say the least.

reply

ziddoap 1 hour ago | root | parent | prev | next [–]

What makes that curious?

reply

jachee 1 hour ago | root | parent | next [–]

Cloudflare's "protection" is basically a racket. e.g.

https://robindev.substack.com/p/cloudflare-took-down-our-web...

reply

dxdm 5 hours ago | parent | prev | next [–]

Maybe it's a form of advertising certain capabilities and services.

reply

neilv 4 hours ago | root | parent | next [–]

IIUC, that's always a good theory for unexplained DDoS. Though, even if they have only profit motivations, I'm a little surprised when they don't seem to let ideology influence their selection of targets for demos.

For the sake of argument (maybe not true), let's say that all techies are aware of archive.org, and consider it beneficial, probably using it themselves.

Why don't they instead demo against a target that will be proof of capability, and one that someone won't pay them to do (no freebies), yet one that they perceive as bad or deserving in some way?

Probably improper to suggest "better" targets here, but I really wonder what's going on when some relative do-gooder gets attacked.

Similarly, ransomware attack on a children's hospital, of all places? Doesn't that get you uninvited to criminal mastermind dinner parties?

As Omar of "The Wire" told us, a man's gotta have a code.

reply

floam 3 hours ago | root | parent | next [–]

One thing to keep in mind m about LockBit ransomeware was it was SaaS — errr RaaS — and there is a good chance the target was picked by an insider there, or it was at least some opportunistic hacker not really associated with those who provided the service, besides signing up as an affiliate.

LockBit was so successful partly because they didn't have to hack anyone themselves. It was basically something advertised "Got SSH or RDP access? Let's make a bunch of money."

This attracted hackers who might not trust themselves to do the extortion part safely, as well as people who didn't actually hack anything but hated their boss, wanted a payday.

reply

fmajid 2 hours ago | root | parent | prev | next [–]

Extortion is usually the motive. "Nice porn/gambling/crypto website you've got here. Shame if something happened to it".

reply

aniviacat 2 hours ago | root | parent | prev | next [–]

Perhaps cruelty is the point.

Perhaps they intentionally attack targets that are generally seen in a positive light, to prove to potential customers that morale is not an issue.

Oh, you want me to DDOS a children's hospital? No problem.

reply

jachee 1 hour ago | root | parent | next [–]

Thus is the power of The Dark Side^W^W^W late-stage capitalism.

reply

prmoustache 2 hours ago | parent | prev | next [–]

My wild guess is most of them are ran by companies offering ddos mitigations services.

reply

DougN7 5 hours ago | parent | prev | next [–]

Maybe there is something damning on there that someone needs kept quiet for a while?

reply

textfiles 4 hours ago | root | parent | next [–]

No.

reply

ai_what 3 hours ago | root | parent | next [–]

> Please don't post shallow dismissals

https://news.ycombinator.com/newsguidelines.html

reply

sirtaj 3 hours ago | root | parent | next [–]

The user you're responding to is Jason Scott of TIA.

reply

ai_what 3 hours ago | root | parent | next [–]

Oh sorry, I guess that makes it a very detailed and well though-out response.

reply

Brian_K_White 3 hours ago | root | parent | next [–]

It does, yes. The single word, from that source, on this topic, communicates all relevant information.

reply

user_7832 1 hour ago | root | parent | prev | next [–]

> Don't be snarky.

Also from https://news.ycombinator.com/newsguidelines.html

reply

Tao3300 2 hours ago | root | parent | prev | next [–]

And regurgitating the rules in a bid to win Junior Mod of the Year is?

reply

Freak_NL 3 hours ago | root | parent | prev | next [–]

That would have been an excellent addition to that comment.

reply

matsemann 1 hour ago | root | parent | prev | next [–]

What's the significance of that?

(Googling "Jason Scott TIA" gives me "Dr Jason Scott is a Senior Research Fellow in the Tasmanian Institute of Agriculture" which doesn't explain much to me)

reply

jkrejcha 30 minutes ago | root | parent | next [–]

Jason Scott works at the Internet Archive[1].

[1]: https://en.wikipedia.org/wiki/Jason_Scott

reply

ziddoap 1 hour ago | root | parent | prev | next [–]

The beauty of acronyms/initialisms that people are too lazy to spell out!

TIA = The Internet Archive (i.e. the victim of the DDoS).

>The user you're responding to is Jason Scott of The Internet Archive

reply

pcdoodle 3 hours ago | root | parent | prev | next [–]

Makes sense: Large media outlets don't like their old BS stories staying accessible. I've seen it used as an accountability tool.

reply

codexon 2 hours ago | parent | prev | next [–]

It's probably because someone saved incriminating evidence on it and they refused to take it down.

reply

swinglock 2 hours ago | parent | prev | next [–]

Are you upset? Can't do nothing about it? It even made a headline or even just a thread on a forum? That's reason enough for some. It could easily be a teenager with no better excuse than not having a fully developed brain and no better reason than liking to ruin things. Having seen how much that happens, I guess it's more likely than a conspiracy or a crime with any rationality behind it.

reply

Joel_Mckay 5 hours ago | parent | prev | next [–]

My thoughts exactly, what is the point of attacking a library... so lame... =/

reply

jauntywundrkind 1 hour ago | parent | prev | next [–]

There are some very bad very shitty people about, just trying to make earth worse.

Npm has been under pretty severe attack for ~6 weeks now. I forget who else.

The scariest thing to me is what we might do in the face of persistent online attacks. If this stuff gets rolled up into western nations rolling back privacy & liberty? That's an theonion.com "bin laden plan to sit back and enjoy collapse" situation. Freak out & let cyber security paranoia reign & destroy free communication & connection.

reply

krapp 1 hour ago | parent | prev | next [–]

Seriously? People do this shit for fun. There used to be a program (LOIC) popular on 4chan used for DDoS attacks all the time, it's the origin of the "firin mah lazer" meme.

reply

viraptor 1 hour ago | root | parent | next [–]

The lazer meme (2006) predates LOIC (~2010) by years https://knowyourmeme.com/memes/shoop-da-whoop

reply

krapp 13 minutes ago | root | parent | next [–]

I stand corrected.

reply

OutOfHere 2 hours ago | prev | next [–]

What are the ways to manage a DDoS attack, preferably using open source? Don't say Cloudflare because they're an extortionist firm.

reply

jsyang00 2 hours ago | parent | next [–]

Cloudflare is not "an extortionist firm". It is a large tech company, where occasionally teams employ shitty sales tactics to meet their numbers, but generally provides a valuable service and acts reasonably ethically.

There are open source tools to mitigate DDoS, but all of them will have some marginal cost to run, and they will all be significantly worse than Cloudflare as they benefit from neither Cloudflare's data moat or scale.

reply

OutOfHere 3 minutes ago | root | parent | next [–]

No, thanks. Cloudflare acts ethically only until it suits them. It is the pre-exploitation phase to lure a customer. We are not fools here.

reply

overstay8930 38 minutes ago | parent | prev | next [–]

Plenty of DDoS mitigation firms use open source tech, but that’s only step one of mitigation, most normal firms will never be able to stop a DDoS attack without someone else with a lot of resources tanks the attack for you.

Even if you go all out and buy a bunch of huge IP transit links, you are not gonna be able to stop the IXP 800 miles away from getting congested and blocking your customers from accessing your site anyways. You need access to a backbone to route traffic differently to avoid those kinds of issues, which is why DDoS scrubbing services will partner with a T1 ISP to do most of the work.

reply

Capricorn2481 2 hours ago | parent | prev | next [–]

I have asked this a few times and never gotten an answer beyond "One day they could turn evil." What is the reason Cloudflare is an extortionist firm? I am way more concerned about Amazon than Cloudflare.

reply

tripletao 1 hour ago | root | parent | next [–]

Beyond the upselling under duress, I've also seen complaints that Cloudflare protects the client-facing websites of DDoS-as-service operators. This enables them to sell their service, which then creates demand for Cloudflare's service from their targets.

Cloudflare describes that policy as a commitment to content neutrality rather than extortion, and I think that's more or less sincere (since they've protected many other unpopular sites that didn't give them such a benefit, with a few high-profile exceptions). It does work out very conveniently for them, though.

reply

remram 1 hour ago | root | parent | prev | next [–]

There was a recent anonymous critic of Cloudflare on the front page: https://news.ycombinator.com/item?id=40481808

reply

Joe_Cool 1 hour ago | parent | prev | next [–]

HAProxy + DDOS protection? https://www.haproxy.com/blog/application-layer-ddos-attack-p...

Or any proof of work proxy that delays the ingress traffic. If you only have one server there is very little you can do except maybe redirect to a static page or kill the DNS entries.

reply

remram 1 hour ago | parent | prev | next [–]

If your application can take it, drop it in the application. If your load balancers can take it, drop it on your load balancers. Otherwise you have to get your provider to drop it, if they can take it. Worse case they'll drop all traffic meant for you to protect the rest of their network.

reply

robertakarobin 2 hours ago | parent | prev | next [–]

Aw darn, they are? I was just considering migrating my frontend to them after seeing all the positive reviews. What's the issue?

reply

markus_zhang 2 hours ago | prev | next [–]

How much $$ does archive.org spend on infra and such? How much does one need to endure the most damaging DDOS? I remember seeing from somewhere that Google went through some huge DDOS attack without going down.

Given its benefit to the lay persons I recommend everyone who use their services give a small amount once for a while. I already did so but if not for family issues I'd donate way more.

reply

mike_d 1 hour ago | parent | next [–]

DDoS attacks are usually volumetric attack. Send more bits than the pipe the website has to the internet.

To combat this you need to buy enough pipes to the internet for your regular internet traffic, as well as an extra 500 Gbps or so. That is a lot of unused bandwidth to be paying for every month. Then once the packets arrive at your datacenter you still need to buy dedicated appliances to scrub out the bad and let the good flow.

Google is constantly under attack, but their normal daily traffic volume (multiple Tbps) is large enough that just the extra capacity they keep on hand to deal with traffic spikes the World Cup or a popular YouTube video is larger than what most attackers can muster.

reply

ChrisArchitect 4 hours ago | prev | next [–]

[dupe]

https://news.ycombinator.com/item?id=40492076

reply

Tao3300 2 hours ago | parent | next [–]

Meta dupe!

https://news.ycombinator.com/item?id=40492670

reply

tetris11 4 hours ago | prev | next [–]

Who's their biggest enemy at the moment

reply

btbuildem 4 hours ago | parent | next [–]

Paywalled sites?

reply

ysofunny 3 hours ago | root | parent | next [–]

let me go further: the whole of the copyrighted industry

including all media conglomerates (obviously) and all scientific, literary, etc, publishing houses.

also, there's a global war, so it well may be a fog-of-war technique or like somebody else also mentioned: someone needs something to stay quite for a little bit as part of some larger operation

reply

markus_zhang 2 hours ago | root | parent | next [–]

The establishment always gets the most advanced technology, attack and defense because they have the big bucks. That's why I never believed that technological advancement promotes individualism, distributed X (whatever X is, money, power, whatever). Eventually it always points to a more centralized world because the elites are able to control more with each technological advancement.

reply

some_furry 3 hours ago | parent | prev | next [–]

That's a tough question to answer without devolving into politics, which is off topic for Hacker News.

I think that's also the wrong question to ask. "Who's doing it?" is less interesting than "What's enabling them to succeed?"

reply

slater 3 hours ago | root | parent | next [–]

Politics isn't fully off-topic on HN; per guidelines, *most* political stuff is off-topic, "unless they're evidence of some interesting new phenomenon"

https://news.ycombinator.com/newsguidelines.html

reply

freitzkriesler2 4 hours ago | prev | next [–]

This is like an arsonist lighting an orphanage or library on fire. Why would you do something like that?

reply

jedberg 4 hours ago | parent | next [–]

To sell your services as an arsonist. Being able to point to a big successful attack helps professional DDoSers sell their services.

reply

ysofunny 3 hours ago | root | parent | next [–]

more cynically, to sell fire-safety insurance

reply

aprilthird2021 3 hours ago | root | parent | prev | next [–]

But wouldn't they need to telegraph the attack in advance to customers? Taking credit after the fact is risky as many competitors will also take credit

reply

jedberg 2 hours ago | root | parent | next [–]

Yes, that is part of it. They tell potential clients, "On May 27th, I'm going to take down the Internet Archive". Then they do it, and then go back to their clients and say, "now that you've seen my work, do you want to pay me?".

reply

aprilthird2021 4 minutes ago | root | parent | next [–]

Then wouldn't it make more sense to take down a target with few eyes on it? Since you're not paid, why deal with the risk of an attack that will make the news?

reply

hnthrowaway0328 1 hour ago | root | parent | prev | next [–]

I wonder where we can find a middleman for that kind of service. Criminal groups would be pretty stupid not paying a middleman to do the checks and filtering.

reply

mandibles 2 hours ago | parent | prev | next [–]

Some people just want to watch the world burn.

reply

freitzkriesler2 1 hour ago | root | parent | next [–]

Precisely no honor amongst thieves.

reply

Tao3300 2 hours ago | parent | prev | next [–]

Probably no good reason. In technical terms, some asshole is dicking around.

reply

1vuio0pswjnm7 23 minutes ago | prev | next [–]

archive-it.org is still working

reply

pixxel 5 hours ago | prev | next [–]

> Sorry to say, archive.org is under a ddos attack. The data is not affected, but most services are unavailable. We are working on it & will post updates in comments.

reply

bhk 5 hours ago | prev | next [–]

Cui bono?

reply

niek_pas 4 hours ago | parent | next [–]

The guy from U2, I think

reply

MobiusHorizons 4 hours ago | root | parent | next [–]

lol, thanks for the good laugh :)

reply

mitchbob 4 hours ago | parent | prev | next [–]

Publishers.

reply

whatsakandr 5 hours ago | prev | next [–]

Clicking this link isn't helping them with their current situation. You'd just be contributing to the ddos.

reply

mttpgn 5 hours ago | parent | next [–]

The link directs to an announcement via "toot" on mastodon.archive.org

reply

DaSHacka 5 hours ago | parent | prev | next [–]

Don't worry, you can visit it through the wayback machine instead!

oh wait

reply

aaomidi 4 hours ago | parent | prev | next [–]

Nope. This should have no impact on the rest of what they're doing.

reply

pmarreck 4 hours ago | prev | next [–]

Is there any way to know who is responsible?

reply

pixelpoet 3 hours ago | parent | next [–]

I think "follow the money" is a decent heuristic here. Why else would anyone do it?

reply

markus_zhang 2 hours ago | root | parent | next [–]

Is it possible for archive.org to trace back the IP addresses? I assume maybe the attackers used a lot of IoT devices or VMs in cloud?

reply

fmajid 2 hours ago | root | parent | next [–]

Botnets usually, sometimes amplification attacks against NTP or DNS, although the Chinese government's Great Firewall also has offensive capabilities known as the Great Cannon, although they are generally used against GitHub because it hosts censorship-circumvention software like VPNs.

reply

markus_zhang 2 hours ago | root | parent | next [–]

Are botnets usually hosted on personal computers or servers or IoT? I'm thinking maybe archive.org can block a whole range of IPs if needed.

reply

0xcde4c3db 2 hours ago | root | parent | next [–]

Resistance to that kind of simple countermeasure is exactly what distinguishes a DDoS attack from a non-distributed DoS attack. The traffic basically comes from "everywhere". Not literally every IP block and route, but widespread enough that it's difficult to separate from legitimate users without actually processing the traffic (which is what you're trying to avoid by e.g. blocking an IP range).

reply

hnthrowaway0328 1 hour ago | root | parent | next [–]

Thanks. And I assume they mostly come from friendly countries which makes it even harder to block?

This is indeed very tough to resist.

reply

rzr 5 hours ago | prev | next [–]

so is purl.org

reply

dang 3 hours ago | prev | next [–]

Url changed from https://bsky.app/profile/archive.org/post/3ktiatctiqm2r, which points to this.

reply

boomboomsubban 5 hours ago | prev [–]

Dupe https://news.ycombinator.com/item?id=40492076

reply